HLDT 03cv

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :	Gavin A. McLintock et al.
Serial No.:	10/004,340
Filed:	October 25, 2001
Title:	DOOR ACCESS CONTROL AND KEY MANAGEMENT SYSTEM AND THE METHOD THEREOF
Docket No.:	34118

LETTER

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Enclosed is a certified copy of Canadian Patent Application No. 2,324,679; the priority of which has been claimed in the above-identified application.

CERTIFIED COPY O
PRIORITY DOCUMEN

Respectfully submitted,

PEARNE & GORDON LLP

By: John P. Murtaugh
John P. Murtaugh, Reg. No. 34226

526 Superior Avenue East
Suite 1200
Cleveland, Ohio 44114-1484
(216) 579-1700

Date: 3-4-02

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner of Patents, Washington, D.C. 20231 on the date indicated below.

John P. Murtaugh
Name of Attorney for Applicant(s)

March 4, 2002 John P. Murtaugh
Date **Signature of Attorney**

1

Office de la propriété intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An Agency of Industry Canada

Bureau canadien des brevets
Certification

Canadian Patent Office
Certification

La présente atteste que les documents ci-joints, dont la liste figure ci-dessous, sont des copies authentiques des documents déposés au Bureau des brevets.

This is to certify that the documents attached hereto and identified below are true copies of the documents on file in the Patent Office.

Specification and Drawing as originally filed with Application for Patent Serial No: **2,324,679**, on October 26, 2000, by **LOCH ISLE INC.**, assignee of Gavin A. McLintock and D. Michael Caughey, for "Method and System for Physical Access Control Using Wireless Connection to a Network".

S. Gregoire
Agent certificateur/Certifying Officer

October 23, 2001
Date

Canada

(CIPO 68)
01-12-00

OPIC CIPO

Abstract

A method and system of physical access control by a key owner to a door controlled by a door controller is disclosed. The key owner is assigned a key which is identified by the door. The door transmits this identification to a remote computer network which then returns a message on whether the key is authorized based on security settings controlled by the door controller. The door then either grants or denies access based on the message.

METHOD AND SYSTEM FOR PHYSICAL ACCESS CONTROL USING WIRELESS CONNECTION TO A NETWORK

Field

The invention relates generally to security systems and particularly to a method and apparatus of physical access control.

Background

Virtually all private residences, businesses and governments employ locks on all exterior doors and many interior doors to control physical access to premises and vehicles and to protect valuable contents and occupants from outsiders. The technology of locks and related security products has developed to provide a very wide range of choices in security levels, locking mechanisms, key types and other features. Available "key" technologies include, among others, various kinds of mechanical keys, magnetically coded swipe cards, so-called "smart" cards with embedded microelectronic devices, plastic or metal cards coded with mechanical holes, short range radio frequency (RF) or infrared (IR) transmitters with coded signals, and various keypad arrangements requiring the user to enter a pre-determined unlocking code.

Presently, keys are generally associated with one or a few doors and access to the keys, and, thereby, the use of the doors, is controlled by the owner of the premises or vehicle to which the door allows access. The current system of lock usage leads to a number of problems both for the owners of premises and vehicles with lockable doors and for individuals. Most individuals are forced to carry and manage a large number of mechanical keys and/or cards and remember a number of passwords or keypad numbers and remembering which key fits which lock can be an issue, especially for keys which

are used infrequently. Lost keys are difficult and time-consuming to replace and may result, in the case of mechanical keys, in a need to replace or re-key all locks with which the keys were associated and if a number of individuals have keys to a single door and one is lost, all key holders must be contacted and provided with new keys.

As well, passwords or keypad numbers can be inadvertently or deliberately revealed, thereby lessening security and usually resulting in a need to re-program the lock to accept a new code. Then when code locks must be re-programmed, all authorized users must be informed of the new code and they must, therefore remember yet another code.

Also, keeping track of who has keys to which doors can be an issue and this becomes more complex, as in many business situations, the more doors and employees there are.

Further, if individuals are permitted to access some parts of a facility but not others, then a multiplicity of keys is required adding to the problems of key management for both business and individual. And temporary access to premises by, for example, cleaning staff or neighbours, is difficult to control and monitor and reduces security.

Access to premises in emergency or potential emergency situations, such as by fire departments in the event of a fire alarm, usually requires forced entry with attendant structural damage and repair expenses.

Most businesses and many homes make use of monitored alarm systems in addition to door locks, requiring individuals both to carry keys for the premises and to remember alarm codes.

Access control systems exist that solve some of the problems by means of wired connections to the doors for which access is being controlled. Some of these systems can communicate between locations via wide area networks. Generally, such systems require special software and computer systems on or near the premises being protected. Often dedicated monitoring equipment and stations are required. These systems are costly to

install and operate and are oriented towards larger organizations. These systems also do not extend to controlling access to locations where wired connections are impractical.

A number of other locking and access control systems have been devised. For example, it is known to employ wireless communication between a secure door and remote site in order to obtain authorization. While these systems are successful in solving or solving some of the problems mentioned above, they are usually too costly or require too much technical support to be of use to private residences or small businesses. In addition, none of the technologies employed thus far address the problems of the individual who must deal with a large number of keys and codes.

Therefore what is needed is an improved system and method for physical access control.

Summary

A method and system for physical access control using wireless connection to a network is disclosed.

According to the embodiments of the invention there is provided a system of physical access control to a door by an individual, the individual being identifiable by a key wherein physical access is allowed to individuals identified by authorized keys, the system comprising: a door control/lock assembly mounted to the door, the door being locked by an electric lock, the door control/lock assembly unlocking the electric lock upon authorization, the door control/lock assembly comprising: an identification device and an embedded computer for identifying the key; and a means of two way communication; and a remote network in two way communication with the means of communication in order to determine the authorization of the key, the network

comprising: a door server database for storing data on which keys are adapted to be authorized by each door.

Other aspects and advantages of the invention, as well as the structure and operation of various embodiments of the invention, will become apparent to those ordinarily skilled in the art upon review of the following description of the invention in conjunction with the accompanying drawings.

Brief Description of the Drawings

Embodiments of the invention will be described with reference to the accompanying drawings, wherein:

FIGURE 1 illustrates one embodiment of system of physical access control according to the teachings of the present invention;

FIGURE 2 illustrates the details of the system of Figure 1;

FIGURE 3 illustrates the details of the door control/locking assembly; and

FIGURE 4 illustrates a method of access control.

Similar references are used in different figures to denote similar components.

Detailed Description

Referring to Figure 1, there is illustrated a system of physical access control according to the teachings of the present invention.

The system comprises a network of door controllers and key owners. Door controllers control the security settings such as authorizations, of the door or doors they own. Key owners are individuals wanting to gain access to doors, access being any passing through the door including both entry and exit. Preferably, each individual is assigned to or owns a single key which is used to gain access to all doors she/he is authorized to. As seen in Figure 1, door controller 10 controls two doors 12, 14 while door controller 20 controls one door 22. Each key owner 30, 40 is one individual identifiable by a key 32, 42 which is used to gain access to all doors in the system. However, each door controller can set the security to each door at her/his discretion. Therefore, door controller 10 has allowed access by the key owner 30 to door 12 and not door 14, while door controller 20 has allowed access by the key owner 30 to door 22. The key owner with a single key can gain access to either door, but not the third. Each door will identify the key owner by the key he is associated with and either allow or deny access as per its security settings controlled by its door controller. The door controller controls these settings for each door via a remote network. As well, door controller 10 has not allowed access by the key owner 40 to either door 12, 14 while door controller 20 has allowed access by the key owner 40 to door 22. Therefore, a door may be accessible by multiple keys and a single key may access multiple doors.

Prior art systems generally assign a key to a particular door. Any individual requiring access to a door requires the assigned key. According to teachings of the present invention, a key is assigned to a particular individual and the individual is identifiable by the key. The individual (key owner) can gain access to any door in the system that a door controller has configured to accept the individual's key. A door controller can configure the security settings of doors he owns or controls on the network via a browser running on a computer. The browser is used to access a secure web site that is dynamically served via server software, which is connected to an encrypted database. The database stores the list of keys that are allowed to open the door or doors owned by the door controller plus

other security settings such as, for example, the times during which a key may open a door. The server software displays the current contents of the database to the door controller and allows him to make changes to the contents of the database.

A single individual may be both a door controller and a key owner.

Referring to Figures 2 and 3, the system provides a door control/lock security assembly 120 in a door 12 in communication with a computer network 110. While the figure illustrates only one door for the sake of clarity, the network may be in two way communication with several doors comprising door control/lock security assemblies. The computer network comprises a key server system 130 and a door server system 140. In general, the door control/lock assembly provides identification of the person wanting to gain access to a particular door to the computer network while the door server provides information on authorized persons for a particular door and the key server provides information on the doors to which each key is authorized.

The communication line with the computer network 10 is preferably via wireless technology.

Each door on the network preferably comprises a door control/lock assembly, a battery for supplying power, an electric door lock and means to unlock the door lock upon authorization.

The door control/lock assembly includes an identification device, an embedded computer, with the appropriate software and a means of communication. The assembly is mounted to a door to which only authorized persons may enter.

The electric door lock used can be any such lock that preferably has low power consumption.

The door control/lock assembly is embedded in or near the electric door lock and can easily be installed by a qualified locksmith without the requirement of additional training.

The identification device or sensor identifies the person or 'key' wishing to gain access to the secured door. The identification device may be a proximity card reader or swipe card reader or any other such device. In a preferred embodiment, the recognition device may be a wireless electromagnetic receiver employing public key cryptography (PKI) technology or other secure communications technology to receive signals from a device carried by the person. Such device may be an electronic key such as a Dallas Semiconductor iButton®, a cell phone, a portable digital assistant (PDA) equipped with digital wireless capability, a personal communicator device, an RF tag device. These tags provide a short range radius frequency signal that is coded to provide identification of the individual. In addition, a biometric recognition device such as thumb-print reader or face-recognition device may be used. Additionally a numeric or alpha-numeric key pad device may be used. The key, then, is any device that can be sensed by the particular identification device used. For example, the identification device used is a numeric key pad, the key would be a numeric code.

Preferably each door in the system uses the same identification device thereby requiring each key owner to own only one key, the key type corresponding to the type of identification device used on the doors. However, each door may employ any device. Any door control/lock may be equipped with more than one identification device to improve security. In such a case, all keys would be required in order for the system to grant access.

The embedded computer in the door works with the identification device and can run the necessary identification/authorization software and communicate this data with the network via the wireless means of communication. The computer comprises a CPU, RAM and local storage in Flash memory. There are a number of known identification/authorization software applications in the art and any suitable one can be used. Preferably a cache is maintained in local memory in encrypted form, of the most

recent and most frequent authorized users of the door. This cache acts to speed up processing and provides back-up capability in the event that the network connection to the database is disrupted in some way.

In a preferred embodiment, the software running on the embedded computer in the door control/lock assembly periodically conducts a self test of its own functionality and records data from the connected system status sensors.

Each door control/lock assembly is provided with a unique identification code that is encoded in hardware and can be accessed by software programs running in the door control/lock assembly and other software programs running in the computer on the network. In addition, a public key/private key arrangement is used that can be updated as required.

Preferably, all components in the door are very power efficient as the door preferably runs on batteries.

The door control/lock assembly further includes a transmitter/receiver as a means of establishing two way communication with a computer network.

The connection between the door control/lock assembly and computer network is preferably a wireless connection. During operation, the door control/lock assembly transmits the identification data read by the identification device to the network and receives messages by the network on whether the identified key is authorized.

Depending upon the situation and environment, either short-range technology, such as Bluetooth™ or a longer distance technology such as a wireless cellular data connection may be used. In a preferred embodiment, all communication lines employ encryption means for added security.

In a preferred embodiment, the network is an IP network connected to the Internet and accessible by the door control/lock assembly via an HTTP server. However, the network can employ any suitable network protocol.

The network also includes a means of wireless communication in order to complete the two way communication between the door control/lock assembly and the network.

The door server on the network includes a database that contains information on individuals (keys) allowed to enter the door according to the identification device being used on each door. This information is in the form of allowed key signatures. The key signatures consist of the unique codes associated with each key and that serve to distinguish it from any other key. These codes will vary depending on the identification device used on the door. As examples, the key signatures could consist of coded numbers that have been magnetically written onto a normal magnet swipe card, if a swipe card reader is used as the identification device. The key signatures could be the unique, hardware embedded serial numbers assigned at manufacture to iButtons® if an iButton® reader is used as the identification device. The key signatures could be public keys of individuals, corresponding to their private keys, if the identification device at the door is to be a signal from a Bluetooth enabled cell phone or PDA carried by the individual. The key signature could be a fingerprint recognition code if the identification device at the door is a fingerprint reader. The key signatures are preferably stored in encrypted form.

Software programs running on the embedded computer in the door, and on the door server on the network work together to provide a number of functions. In particular, the door server records all uses of the door lock, including authorized entries and unauthorized attempts to enter.

The software running on the door server may also provide the necessary controls and communications capability to allow the door controller to configure many security settings of the operation of the door control/lock assembly in addition to the basic

authorization settings of which keys are allowed to unlock the door. This includes such functions as to who is authorized at specific times. Other additional functions include settings as to who is to be notified in the event of an alarm low battery condition or hardware failure condition being detected and how such notification is to take place (e.g.: email, pager, automated phone call, etc.) Such factors as the amount of lead time to report low battery condition can also be set.

In a preferred embodiment, the software running on the door server on the computer network periodically polls all connected door control/lock assemblies to update frequent or most recent users and receive reports from the embedded computer system self-test routines. If the embedded computer in the door control/lock assembly does not receive a poll from the door server within a pre-set interval, it initiates a report to the server on its own.

A single door server may provide these functions for a number of doors controlled by the same door controller or multiple door servers may be used. The same door server may also provide these functions for a number of different door controllers, but each door controller is prevented from accessing the information pertaining to doors controlled by others. Any number of door servers may run on the system at the same time. The information recorded in each door server database concerning the authorized entrances and exits through the door and the unauthorized attempted entrances and exits may be used in any of several ways. Reports may be generated immediately or historically and direct connection may be made to other software systems.

The key server on the network includes a database that contains information on the door to which each individual (key) is allowed access. Software programs running on the embedded computer in the door and on the key server on the computer network work together to provide a number of functions. In particular, the key server records all use of the key, including authorized entries and attempts to enter using the key that were not authorized on a door-by-door basis.

The information recorded in the key server database concerning the uses of the key to unlock various doors and any unauthorized attempted entrances and exits may be used in any of several ways. Reports may be generated immediately or historically and direct connection may be made to other software systems.

The key server may further provide the key owner with reports of every instance of the use of his key(s) that has been recorded anywhere on the network.

A single key server may provide these functions for a number of keys owned by the same key owner. This multiplicity of keys may be keys of the same type or of different types. The same key server may also provide these functions for a number of different key owners but each key owner is prevented from accessing the information pertaining to keys owned by others.

The door server and key server databases on the network can be updated and viewed from any browser. Preferably this is over a secure, password protected link. Generally, a door controller has read and write access to doors he controls while a key owner only has read access to doors he has access to and write access to his key server. Software programs communicate between the embedded computer in the door and the databases on the network and provide the authorization, entry recording and other functions.

Since the door server and key server both maintain logs of entries and exits, it is possible to access the database and determine whether anyone is in the secured area, and if anyone is indeed in the area, the identity of the person.

The disclosed system and method provides a security means to control access by persons to building, rooms or vehicles, while gathering useful information. The system provides a means to allow a person access to some locations, and while exclude access to other locations while allowing the use of only one access key per individual. Such access privileges may be variable according to time. The system provides a means to change the security settings such as access privileges of an individual quickly and easily from

any location where an Internet connection and browser software are available. Information gathered by the system includes the time of all attempts to access the door and the identification of the individual attempting such access (if known) or the fact that an unknown individual attempted to gain access. Furthermore the access privileges associated with the 'key' may be easily changed as circumstances change. This allows people potential to have only one 'key' to open all of the doors in their lives while, at the same time, increasing security and convenience.

Referring to Figure 4, there is illustrated a method 400 for controlling physical access according to the system described above.

In step 410, a key is assigned to an individual or key owner. In step 420, a door controller sets the security settings for door controlled by him. In step 430, the key owner tries to gain access to a door in the system. In step 440, the door identifies the key and key owner. In step 450, the door transmits this data to the network. In step 460, the network responds with information on the authorization settings for the door. The key identification information, along with door identification information and the time of the access request, all in encrypted form, are received by the door server software, decrypted, and compared with the list of authorized key signatures in the database for the door. If a match is found, a return signal is sent to the door, over the network, also in encrypted form, authorizing the door to be unlocked. The information that an access request was made and granted, or not in the case that no matching key signature was found in the database, is added to the database for later perusal or other use by the door owner. In step 470, the door either grants or denies access based on the received information. On receipt and decoding of a message authorizing entry, the door control circuitry sets a switch to energize a standard electronic lock mechanism to unlock the door for a pre-determined period of time (which may be set by the door owner using the browser interface, such setting is also stored in the encrypted database). The door control then sends a confirming message over the network to the door server software, indicating successful receipt of the unlocking message and the unlocking of the door. If the door is equipped with a door

open sensor, the information on whether the door is actually opened or not is also sent to the door server software for storage in the database.

To deal with the occasional instance that the network is not available and to speed up access for frequent users of a door, a small database of frequent and most recent users authorized key signatures is stored in encrypted form in the door controller itself. Before sending a request message for authorization over the network to the door server software, the door control checks its own, internal database and unlocks the door if a match is found between the signature of the key being presented and one that is stored in the database. The information that this action has taken place is then transmitted to the door server software for storage subsequent to the door having been unlocked. Periodically the authorized keys in the door controller local database are confirmed between the door controller and the door server software by a series of encrypted messages over the network. This confirmation process may be initiated by the door controller or the door server software. If a key signature that was authorized is no longer authorized, its status having been changed by the door owner, then the key signature is removed from the door controller local database by the door controller.

Referring now to specific uses and embodiments of the invention, additional benefits and advantageous features will be appreciated. The following optimal and alternative embodiments are provided as exemplifications to aid in appreciating the invention but are not to be considered necessarily limitations on the scope of protection claimed.

Alternative Embodiments

The door control/lock assembly may include other components to provide additional functions. Such a device may be a microphone and speaker assembly to act as a doorbell/intercom. This works by communicating with the software in the door server computer on the network, which then communicates with designated persons or other

systems using email, telephone or pager according to instructions included in the door server.

A doorbell/intercom signalling device is preferably configured to send a message via email, pager or telephone to an individual designated in the network database as the monitoring individual. The designated monitoring individual may be located anywhere that an Internet connection and browser software are available. The designated monitoring individual may be easily changed or such changes may be pre-scheduled. Multiple monitoring individuals may be designated.

As well, wireless alarm devices such as motion detectors, smoke detectors, water detectors etc. may be installed. The wireless alarm device communicates with the software in the door server on the network which in turn communicates the alarm conductor according to instructions included in the database. Any added alarm components, preferably, are configured to signal their condition in flexible ways and to monitor multiple locations that can be altered easily over time.

The door control/lock assembly may further include a sensor that detects whether the door is open or closed. A buzzer device may also be included. If the door remains open for a period of time longer than a pre-set interval, then, the buzzer is sounded for a brief period before an alarm condition message is sent to the individual or individuals designated in the door server database to deal with such alarms. If the door is closed after the sounding of the buzzer but before the sending of the alarm message, the alarm is not sent. Alternatively, the buzzer is not sounded and the alarm condition message is sent immediately. In either case, the information that the door open alarm condition was encountered is stored in the door server as a reporting function. The pre-set interval for which the door may remain open before the buzzer sounds may be changed and may vary with time of day or it may be disabled for specific periods to accommodate various situations. Any such changes or scheduling are accomplished by the door controller accessing the door server via a browser, as is the selection of the buzzer option.

Other system status sensors that may be part of the door control/lock assembly include a battery voltage sensor and a temperature sensor.

The door control/lock assembly communicates with a remote computer network, which is preferably at least partly on the Internet. The network includes a door server and a key server on at least one computer which runs a standard secure web server program as well as the network component of the door locking software, the door server database, key server software, key server database user interface scripts and appropriate reporting, signalling and control software for the system.

However the key server software and the key server database may alternatively be on a separate computer on the network. In this case, the second computer would also run a standard secure web server program, user interface scripts and appropriate reporting, signalling, and control software for the system.

The means of wireless communication may include Bluetooth™ wireless communications circuitry and a network access module consisting of Bluetooth™ wireless communications circuitry, an ethernet network interface and a battery backed up power supply. The network access module is located at a convenient ethernet port within the range of the Bluetooth™ wireless communications circuitry. This module provides the connection between the network and the door lock for exchanging information regarding authorization for access.

Alternatively, the means of wireless communication may include digital cellular wireless Internet access circuitry to provide greater range or for use where an ethernet network port is not convenient.

Alternatively the means of wireless communication may use Wireless Access Protocol (WAP) technology or any other wireless Internet access technology for communications.

In a preferred embodiment, all communication is conducted over encrypted communication lines.

The system may also include a digital camera (still or video) that is configured to provide an image of the individual attempting to gain access to a person assigned to make human judgements on whether such individuals, not identified by the system should be allowed access. The judging person may then allow the individual in, if desired, by signalling the door control/lock assembly from a browser. The camera may also be configured to record in the network databases, an image of all individuals attempting to gain access.

The door control/lock assembly may further be installed on a vehicle door rather than a building door. In this case, a battery power supply is not required, nor would a doorbell/intercom signalling device. An alarm system could be installed, however, the alarm system need not be wireless.

Examples of Uses for the Disclosed System

The disclosed system may be used on any door requiring access control. In addition to building doors, both external and internal, it may be used on a vehicle door. The door controller for the vehicle (presumably the vehicle owner) may set various settings to control access to the vehicle.

A special case exists for use in hotels, where the disclosed system allows the potential for hotel guests to avoid registering at the front desk. Instead, they can proceed directly to their rooms where 'registration' occurs as they are recognized at the hotel room door via their pre-arranged access identification or 'key'. The network databases may be connected to the hotel guest reservation and registration system.

Fire Departments and other emergency crews can be allowed easy access to a building in emergency situations if door controllers authorize the use of a Fire department key.

Emergency workers can also be allowed access to information on the door server which allows them to determine with much greater certainty whether anyone is actually in a burning building.

Many home owners with pets can configure a residential door to be operable by the pets themselves such to allow the pets access to and from the house while still providing security against access by other animals or by human intruders. A key can be assigned to allow the pet to use a pet door at will while keeping it locked to others. Times of operation can be set by the pet owner via a browser. Via the browser, as well, the pet owner can be informed as to whether the pet is in or out, how may times the pet has gone in/out etc. An example of such a key is an RF tag device. These tags provide a short range radius frequency signal that is coded such that the animal (and possibly its owner) can be identified by reference to a registry of such tags. The tag may either be implanted or mounted in a pet collar.

The previously described embodiments of the present invention have many advantages including:

If a 'key' is lost or stolen it can be quickly and easily replaced for all its uses with no chance that the lost or stolen 'key' may be used by unauthorized persons. Attempts by someone to use the lost or stolen 'key' can be reported to the key server database owned by the rightful key owner and such information may be useful in locating the missing key and possibly in apprehending the thief.

The system permits line ups at hotel check ins or car rental agencies to be avoided while ensuring security for both the patron and the hotel or car rental agency. As well, keys not returned to hotels or car rental agencies are an expense and a potential security problem. The disclosed system removes both the expense and the security threat.

Further, in a hotel with this system installed, hotel staff have the means to know if someone is in a room without disturbing the occupant. The need for 'do not disturb' signs is eliminated and hotel guests will be disturbed much less frequently.

When a employee is terminated or quits a position, keys which are not returned to the employer are an expense and a potential security threat. This system removes both the expense and threat.

With the addition of optional components, such as alarm system components, a digital camera or a doorbell/intercom signalling device security may be further enhanced.

The disclosed system may be retro-fitted in many situations resulting in a lower cost of installation.

The system has a lower cost of operation than a highly complex current system.

No special user software is required. The required software systems run within the doors for which access is being controlled and on servers that may be run by third party service providers.

Information logs on use of the physical access control system is recorded remotely from the door over the network.

There is no physical limit to the number of individuals that can be granted access to any door on the system since the databases are remotely stored on a computer on the network.

The system allows the possibility for individuals to have one key that can be used for multiple situations, including their residences, various work situations, vehicles or any other places to which they may need access on a regular or occasional basis. These

access privileges can be altered or scheduled easily and quickly to apply to specific times or to adapt to changing circumstances. Such changing circumstances may include moving to a new house, acquiring vacation property, changing jobs, acquiring a new vehicle, renting a vehicle, renting a hotel room, temporarily accessing the house of a friend or neighbour, or losing a 'key'. In the case of a lost or stolen 'key' (where biometric identification systems are not being used) the old key can be cancelled for all of its uses and a new 'key' can be authorized quickly and easily from any place where an Internet connection and browser software are available.

While the invention has been described according to what are presently considered to be the most practical and preferred embodiments, it must be understood that the invention is not limited to the disclosed embodiments. Those ordinarily skilled in the art will understand that various modifications and equivalent structures and functions may be made without departing from the spirit and scope of the invention as defined in the claims. Therefore, the invention as defined in the claims must be accorded the broadest possible interpretation so as to encompass all such modifications and equivalent structures and functions.

What is claimed is:

1. A system of physical access control to a door by an individual, the individual being identifiable by a key wherein physical access is allowed to individuals identified by authorized keys, the system comprising:

a door control/lock assembly mounted to the door, the door being locked by an electric lock, the door control/lock assembly unlocking the electric lock upon authorization, the door control/lock assembly comprising:

an identification device and an embedded computer for identifying the key; and

a means of two way communication; and

a remote network in two way communication with the means of communication in order to determine the authorization of the key, the network comprising:

a door server database for storing data on which keys are adapted to be authorized by each door.

2. A system of physical access control as claimed in claimed in claim 1, wherein the network or part thereof is the Internet accessible via a web browser.

3. A system of physical access control as claimed in claim 2 wherein the system provides physical access control to multiple doors by multiple keys, each door being

configurable to authorize multiple keys and each key is adaptable to be authorized by multiple doors.

4. A system of physical access control as claimed in claim 3 wherein the network further comprises:

a key server database for storing data on which doors are configured to authorize each key.

5. A system of physical access control as claimed in claim 4 wherein each door has a door controller, each door controller having control to configure which keys are authorized, each door controller being able to configure each door via a web browser.

6. A system of physical access control as claimed in claim 2 wherein the door is configurable to various security settings, the security settings being configurable via the web browser.

7. A system of physical access control as claimed in claim 2 wherein the door control/lock assembly comprises:

means to transmit and to receive a messages from the databases on whether the identified key is authorized.

8. A system of physical access control as claimed in claim 2 wherein the door is a vehicle door.

9. A system of physical access control as claimed in claim 4 wherein the door server and key server are on a single computer on the network.

10. A system of physical access control as claimed in claim 4 wherein the door server and key server are on different computers on the network.

11. A system of physical access control as claimed in claim 7 wherein the identifying means includes an identification device, and the transmitting and receiving means is a wireless transmitter/receiver.

12. A system of physical access control of multiple key owners to multiple doors, each door being controlled by a door controller, each key owner being identifiable by a different key, each door allowing physical access only to key owners identified by authorized keys, the system comprising:

means for each door controller to control which keys are authorized to their doors;

means for each door to identify each key owner by their key; and

means to allow access by key owners identified by authorized keys, each key being capable of being authorized by multiple doors.

13. A system of physical access control as claimed in claim 12 the system further comprising a remote network in two way wireless communication with each door in order to determine the authorization of a key.

14. A system of physical access control as claimed in claim 13, wherein the network or part thereof is the Internet accessible via a web browser.

15. A system of physical access control as claimed in claim 13, wherein the network comprises:

a door server database for storing data on which keys are adapted to be authorized by each door; and

a key server database for storing data on which doors are configured to authorize each key.

16. A system of physical access control as claimed in claim 15 wherein the door server and key server are on a single computer on the network.

17. A system of physical access control as claimed in claim 15 wherein the door server and key server are on different computers on the network.

18. A system of physical access control as claimed in claim 14 wherein the means for each door controller to control doors controlled by each door controller is done via a web browser.

19. A method of controlling physical access to a door by the system of claim 2 comprising the steps of:

assigning a key to the individual;

the door identifying the individual by the key;

the door transmitting the identification to the network; and

the door receiving a message from the database on whether identified key is authorized.

20. A method of controlling physical access as claimed in claim 19 further comprising the step of configuring each door as to which keys are authorized via a web browser.

21. A system of physical access control comprising:

at least one door to be controlled comprising:

a door control/lock assembly comprising:

an identification device;

an embedded computer working with the identification device to identify an individual wanting access; and

a wireless transmitter/receiver;

an electronic lock for restricting access, the door control/lock assembly unlocking the electric lock upon authorization.; and

a battery pack for supplying power to the door components; and

a remote network comprising:

a door server database for storing data on which keys are adapted to be authorized by each door;

a key server database for strong data on which doors are configured to authorize each key; and

a wireless transmitter/receiver for communicating with the door's wireless transmitter/receiver in order to determine the authorization of the individual wanting access.

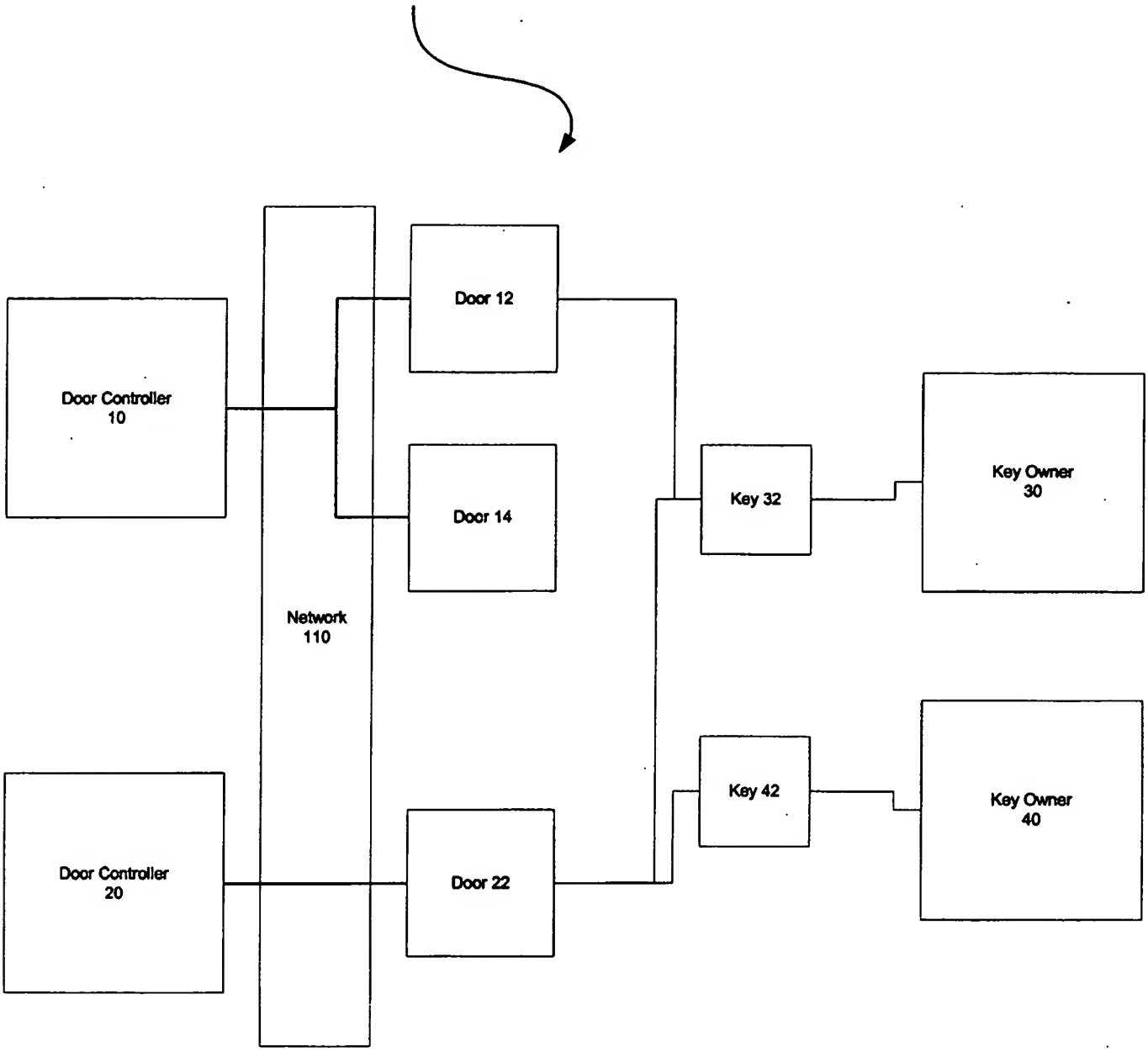

100
Door Controller
10
Door 12
Door 14
Network
110
Key 32
Key Owner
30
Door Controller
20
Door 22
Key 42
Key Owner
40

Figure 1

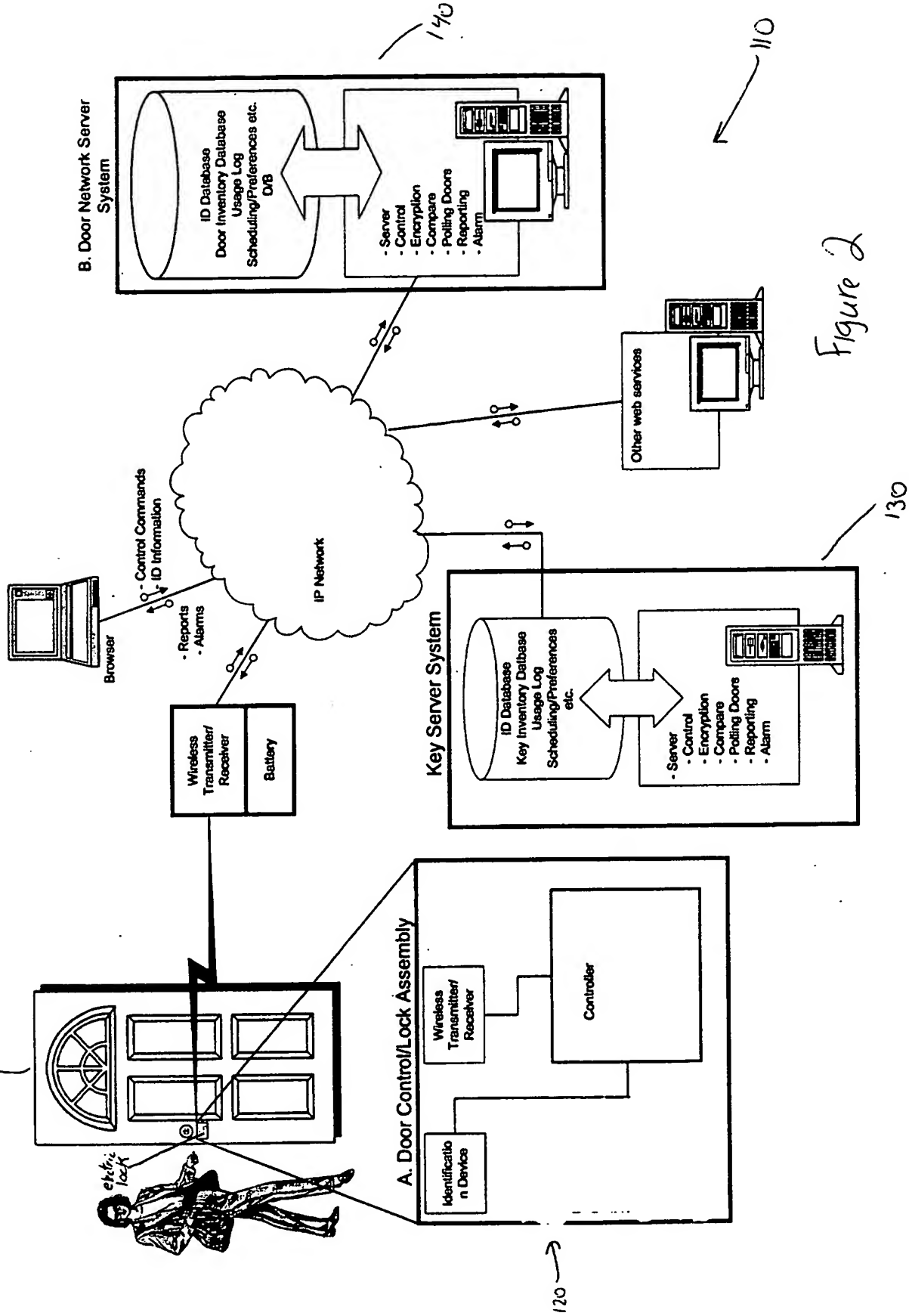
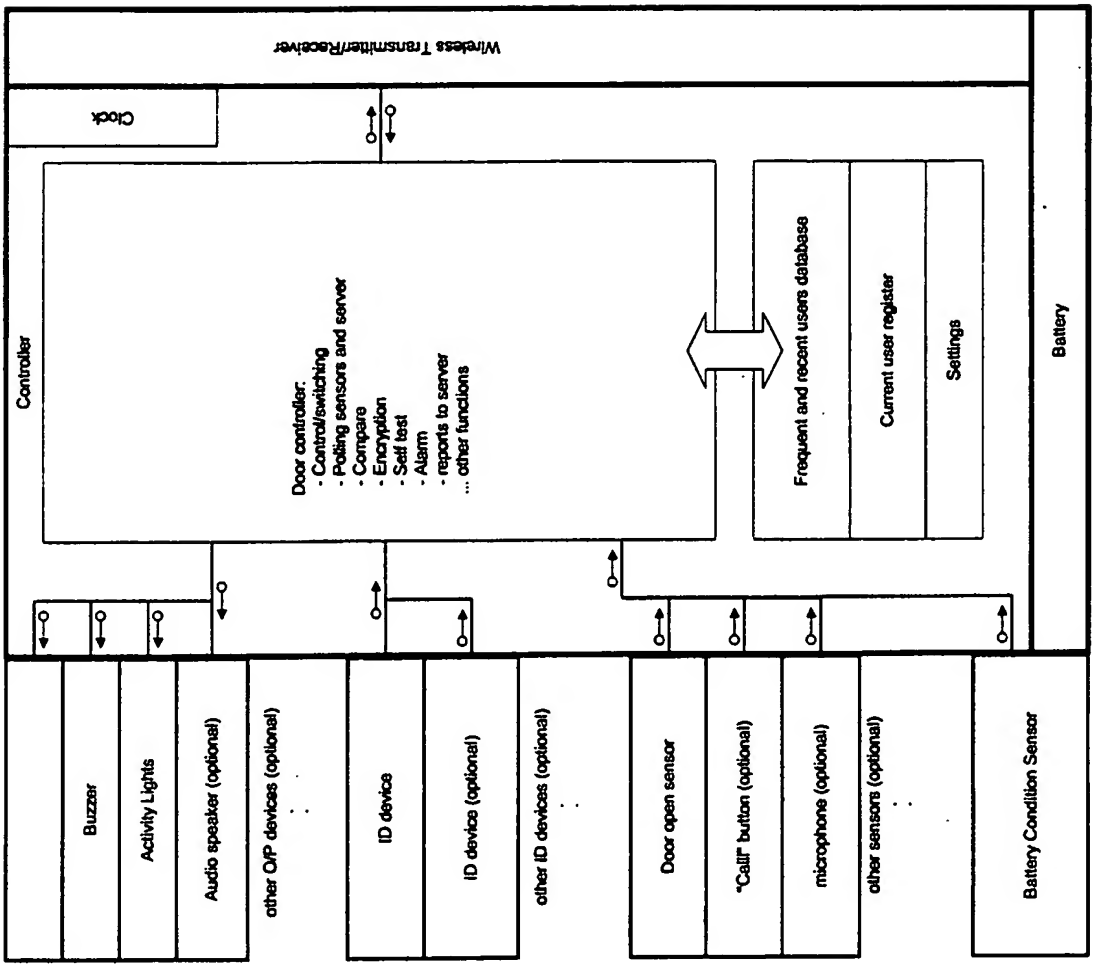

140
110
B. Door Network Server System
ID Database
Door Inventory Database
Usage Log
Scheduling/Preferences etc.
DVB
- Server
- Control
- Encryption
- Compare
- Polling Doors
- Reporting
- Alarm
Other web services
IP Network
- Control Commands
ID Information
- Reports
- Alarms
Browser
130
Key Server System
ID Database
Key Inventory Database
Usage Log
Scheduling/Preferences etc.
- Server
- Control
- Encryption
- Compare
- Polling Doors
- Reporting
- Alarm
Wireless Transmitter/ Receiver
Battery
12
electric lock
A. Door Control/Lock Assembly
Wireless Transmitter/ Receiver
Controller
Identification Device
120

Figure 2


Wireless Transmitter/Receiver
Clock
Controller
Door controller:
- Control/switching
- Polling sensors and server
- Compare
- Encryption
- Self test
- Alarm
- reports to server
... other functions
Frequent and recent users database
Current user register
Settings
Battery
Buzzer
Activity Lights
Audio speaker (optional)
other O/P devices (optional)
ID device
ID device (optional)
other ID devices (optional)
Door open sensor
"Call" button (optional)
microphone (optional)
other sensors (optional)
Battery Condition Sensor

120

Figure 3

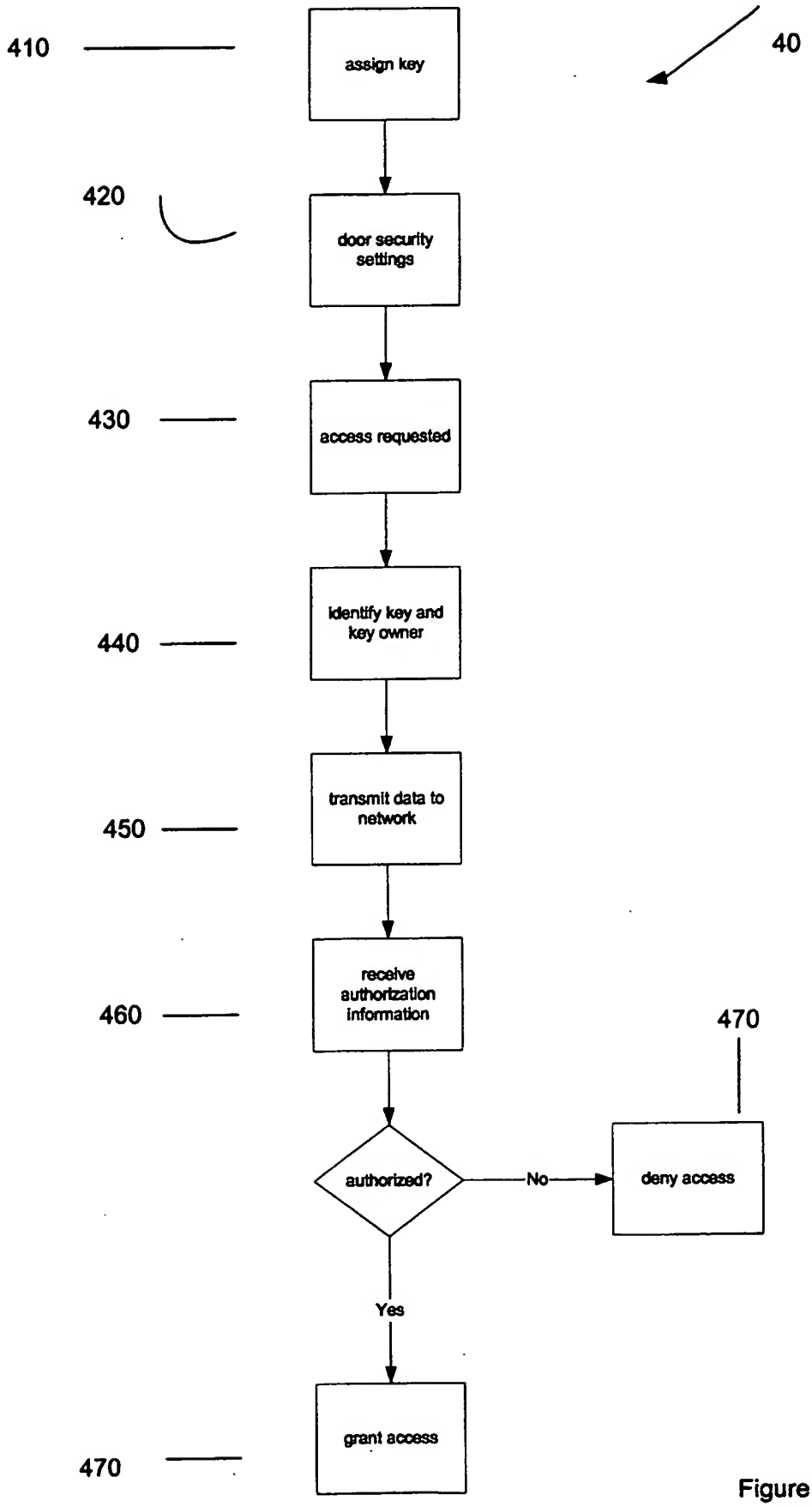

40
410
assign key
420
door security settings
430
access requested
440
identify key and key owner
450
transmit data to network
460
receive authorization information
470
authorized?
No
deny access
Yes
grant access
470

Figure 4